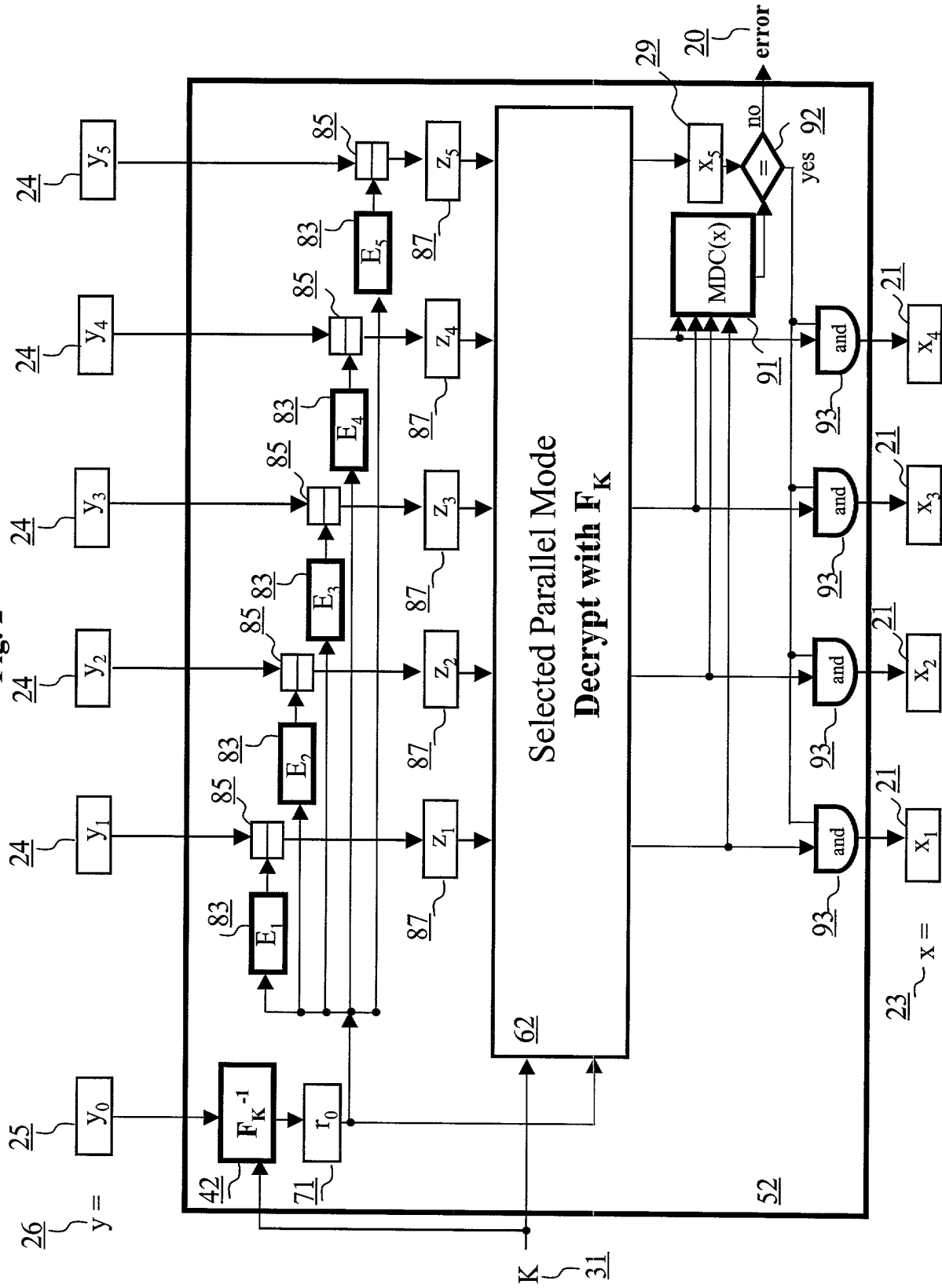


Fig. 2



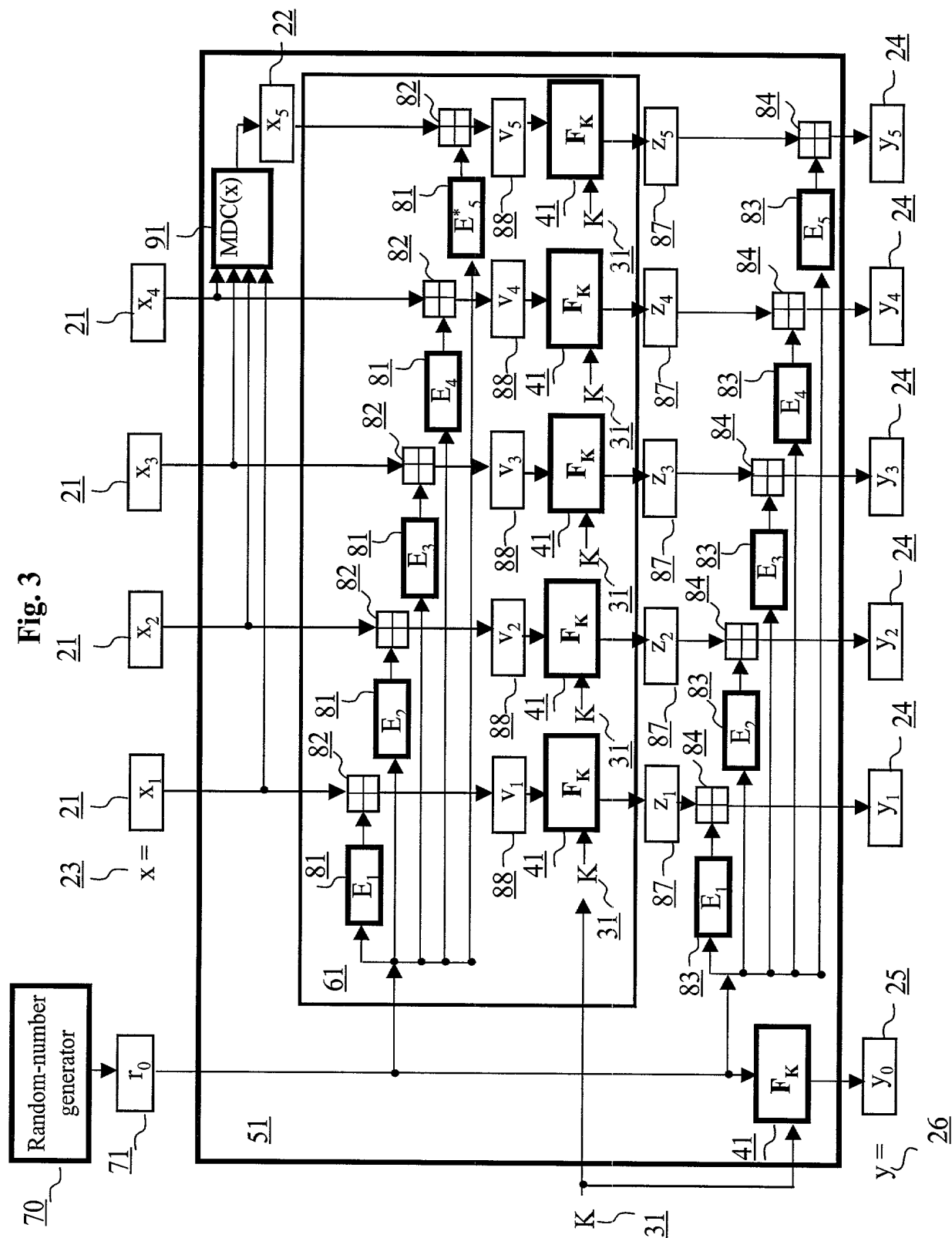


FIG. PARALLEL BLOCK ENCRYPTION
METHOD AND MODES FOR DATA
CONFIDENTIALITY AND INTEGRITY
PROTECTION

Inventor(s): Virgil D. GLIGOR et al.
DOCKET NO.: 068398-0107

Fig. 4

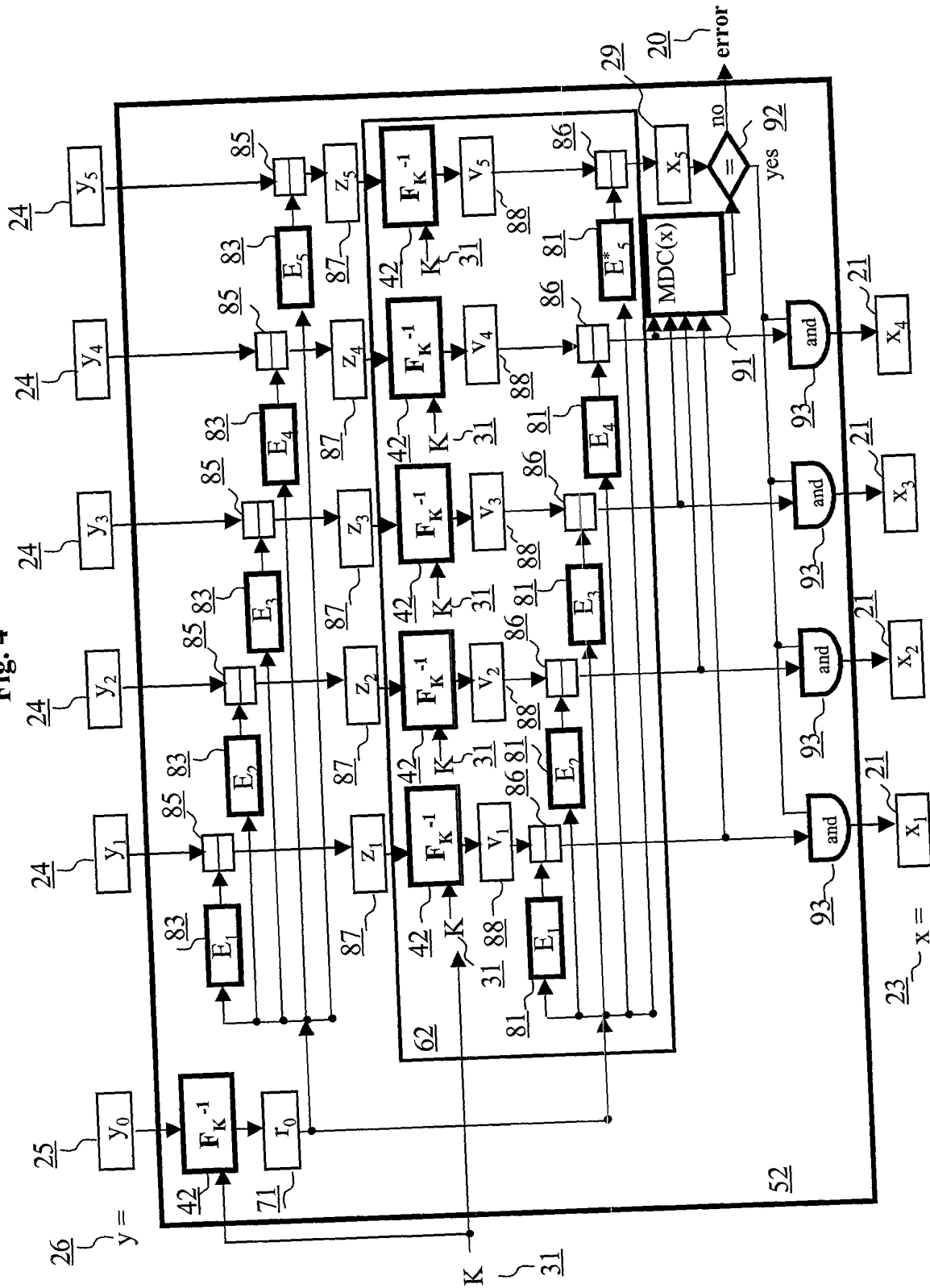
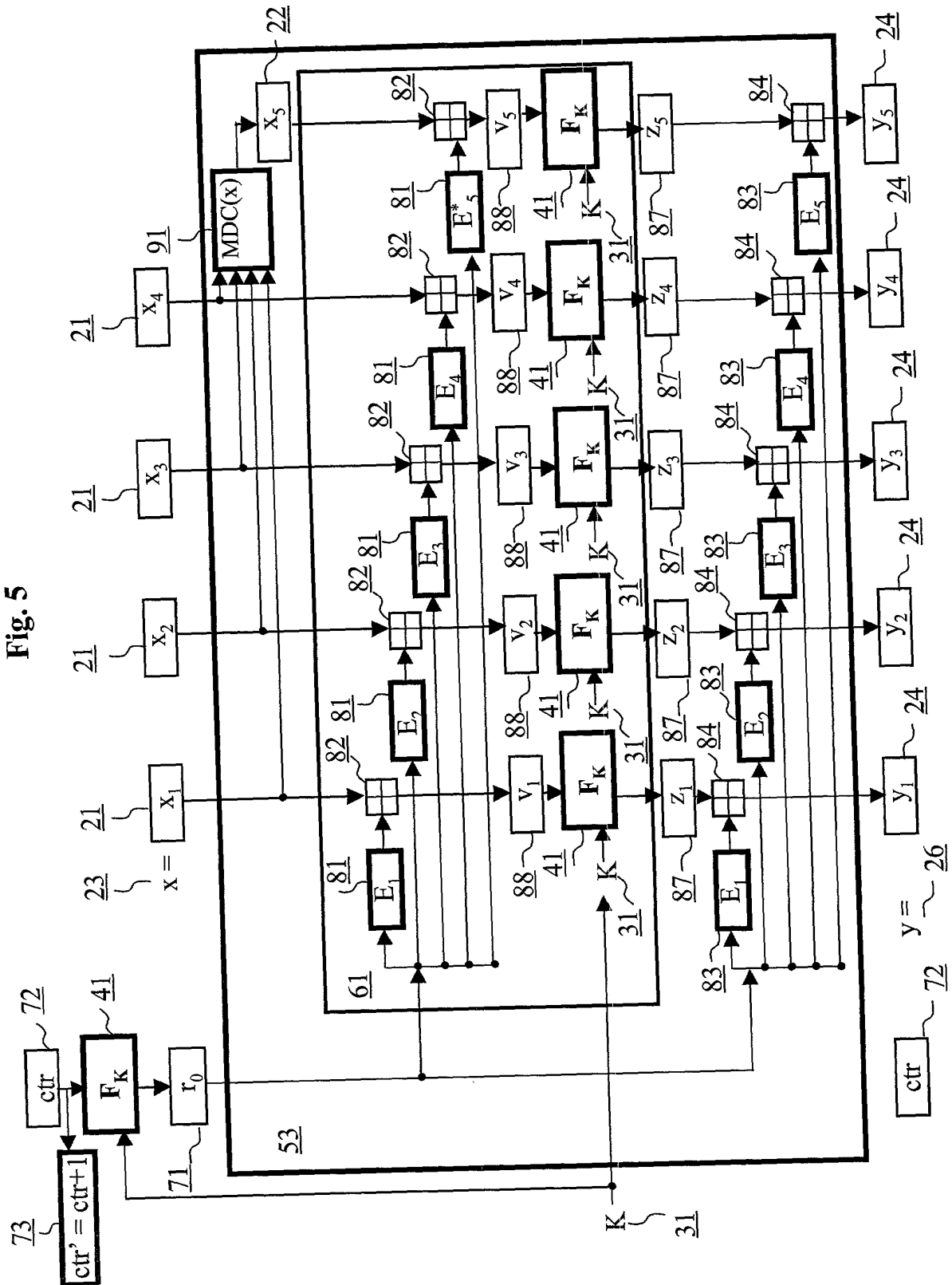


Fig. 5



THE PARALLEL BLOCK ENCRYPTION
METHOD AND MODES FOR DATA
CONFIDENTIALITY AND INTEGRITY
PROTECTION

Inventor(s): Virgil D. GLIGOR et al.
DOCKET NO.: 068398-0107

Fig. 6

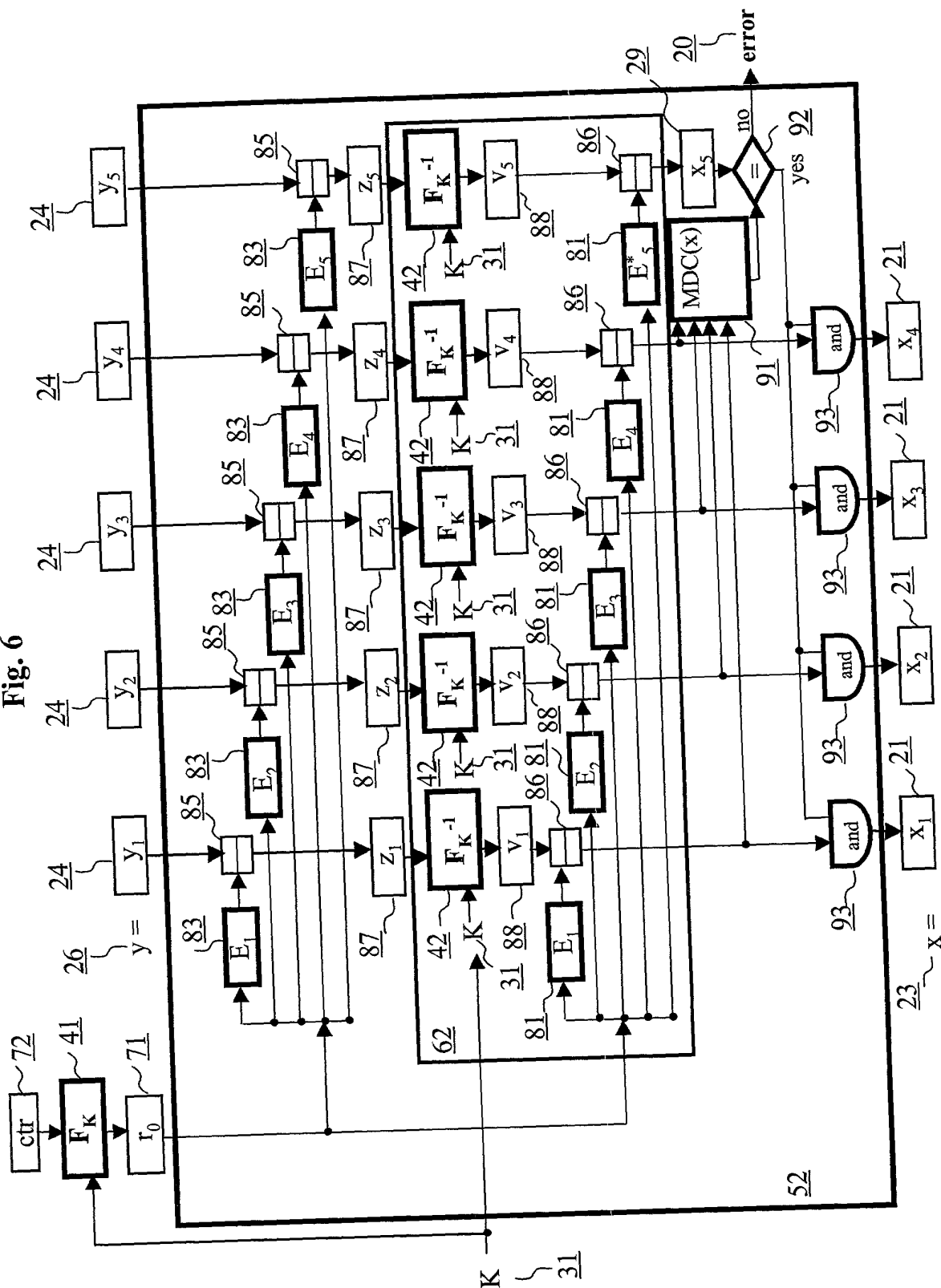


Fig. 7

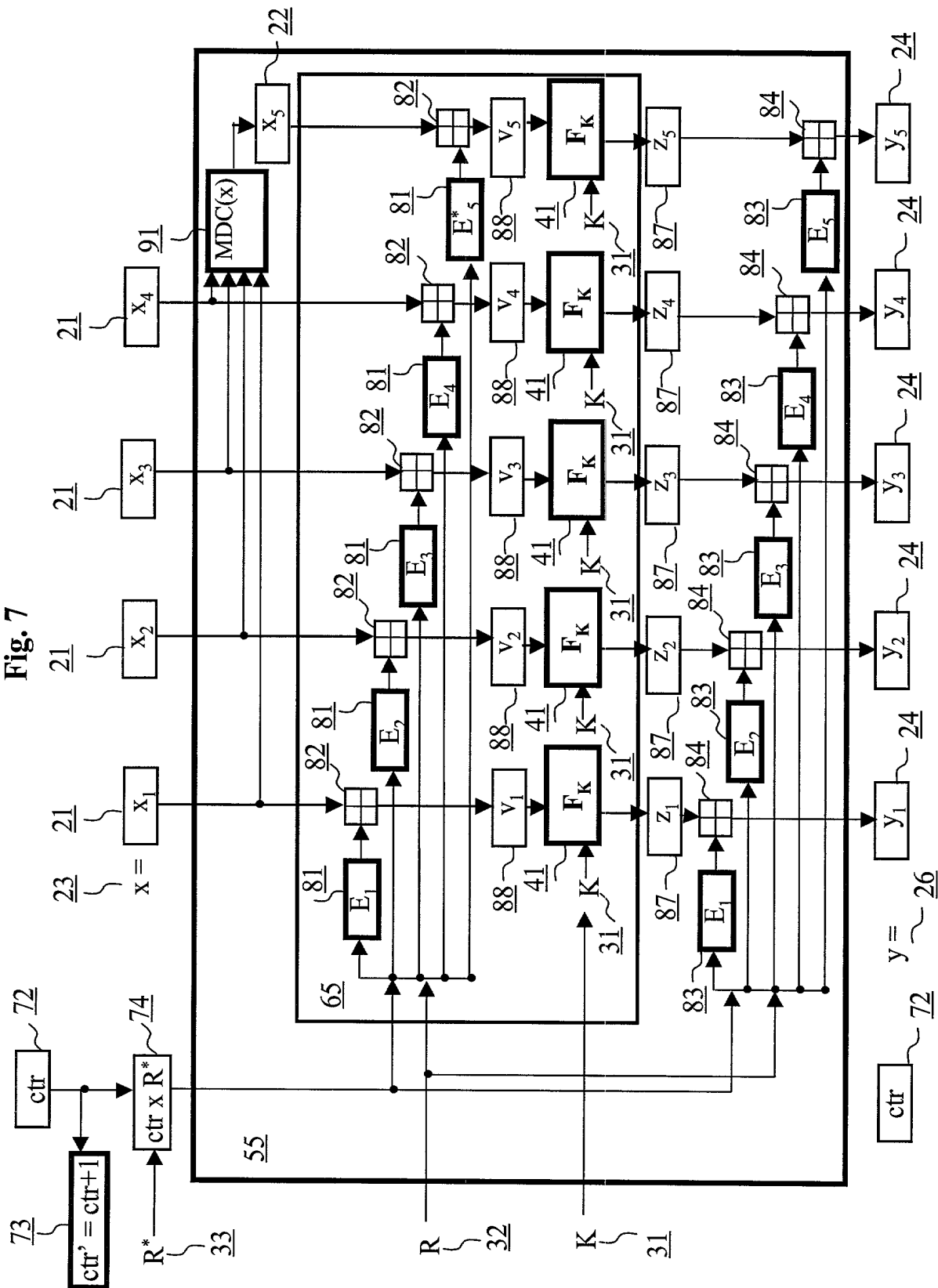


Fig. 8

The diagram illustrates a cryptographic system 56. It starts with a counter ctr (72) and a counter increment block $ctr' = ctr + 1$ (73). The counter is used to generate a key stream R^* (33) and a counter value $ctr \times R^*$ (74). The key stream R^* is combined with a key K (31) to produce a key schedule K (32). The key schedule K is used to generate a series of key components K_1, K_2, K_3, K_4, K_5 (42). These key components are used in a series of processing blocks E_1, E_2, E_3, E_4, E_5 (83) to process a vector $y = [y_1, y_2, y_3, y_4, y_5]$ (24). The output of these blocks is a vector $z = [z_1, z_2, z_3, z_4, z_5]$ (87). The vector z is then processed by a final block F_K^{-1} (42) to produce a vector $v = [v_1, v_2, v_3, v_4, v_5]$ (31). The vector v is then combined with the counter value $ctr \times R^*$ (74) to produce a final output $x = [x_1, x_2, x_3, x_4, x_5]$ (21). The system also includes a feedback loop for the counter and a final output block.

Fig. 9

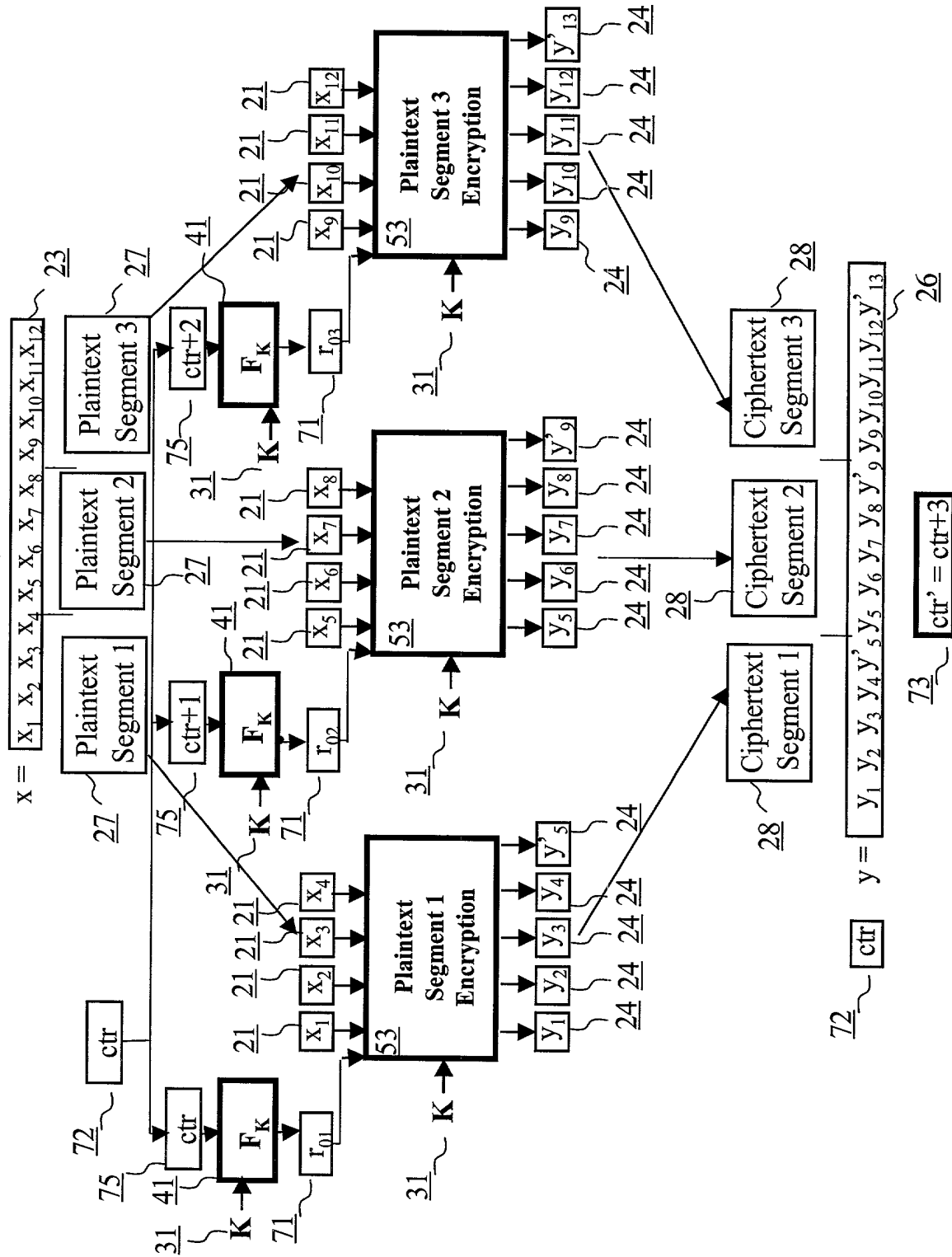


Fig. 10

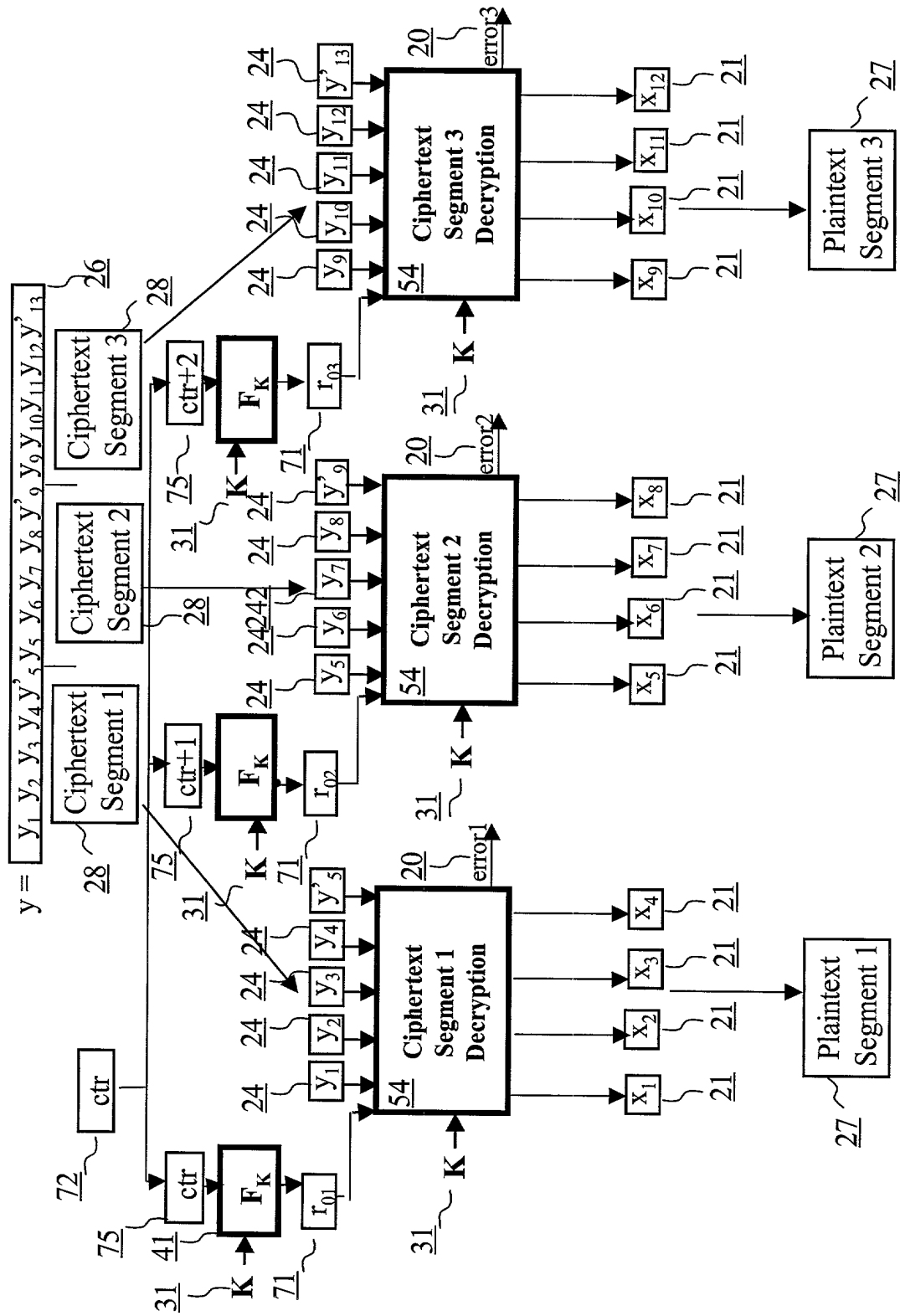


Fig. 11

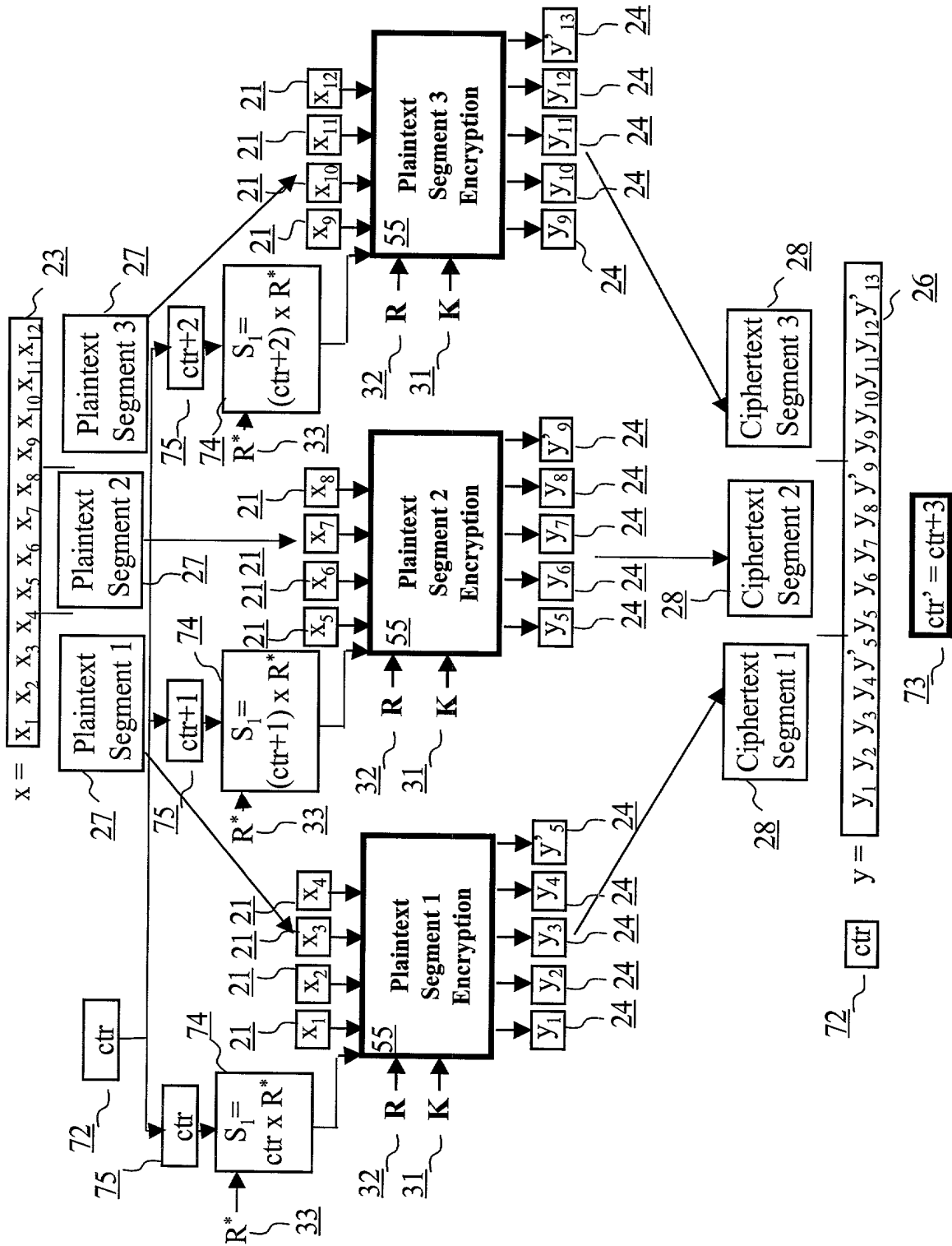


Fig. 12

